

PATENT ABSTRACTS OF JAPAN

(11)Publication number: 09-179726

(43)Date of publication of application: 11.07.1997

(51)Int.Cl.

G06F 7/58

(21)Application number: 07-336920

(71)Applicant: NEC CORP

(22)Date of filing: 25.12.1995

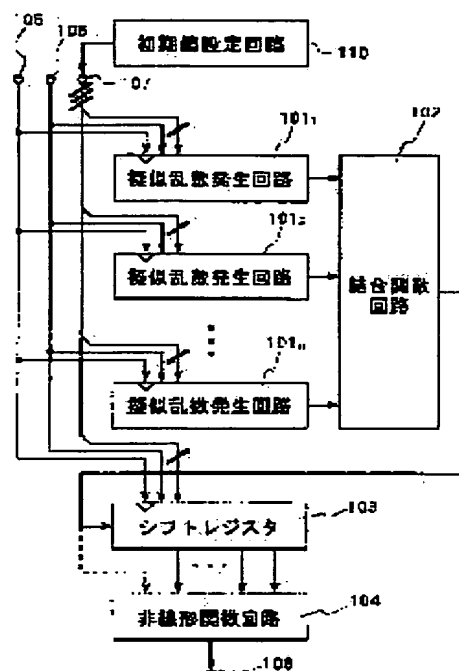
(72)Inventor: SHIMADA MICHIO

(54) PSEUDO RANDOM NUMBER GENERATOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a pseudo random number generator suitable for stream ciphers by generating a nonlinear large pseudo random number sequence by a pseudo random number generation circuit.

SOLUTION: An initial state setting circuit 110 is connected so as to set the bit sequence of an initial state to respective pseudo random number generation circuits 1011-101n and a shift register 103. In the case of generating pseudo random numbers, the initial state of the pseudo random number generation circuits 1011-101n and the shift register 103 is supplied to an input terminal 107 by an initial value setting circuit 110. Then, '0' is supplied to the input terminal 106 and one control pulse is inputted to the input terminal 105. As a result, the initial state is set to the pseudo random number generation circuits 1011-101n, and the shift register 103. Then, when '1' is supplied to the input terminal 106, the pseudo random numbers are obtained bit by bit from an output terminal 108 every time one control pulse is inputted to the input terminal 105 thereafter.



LEGAL STATUS

[Date of request for examination] 25.12.1995

[Date of sending the examiner's decision of rejection] 18.08.1998

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's]

decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-179726

(43) 公開日 平成9年(1997)7月11日

(51) Int.Cl.⁶

識別記号

庁内整理番号

F I

技術表示箇所

G 0 6 F 7/58

G 0 6 F 7/58

A

審査請求 有 請求項の数 6 O L (全 10 頁)

(21) 出願番号

特願平7-336920

(22) 出願日

平成7年(1995)12月25日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 島田 道雄

東京都港区芝五丁目7番1号 日本電気株式会社内

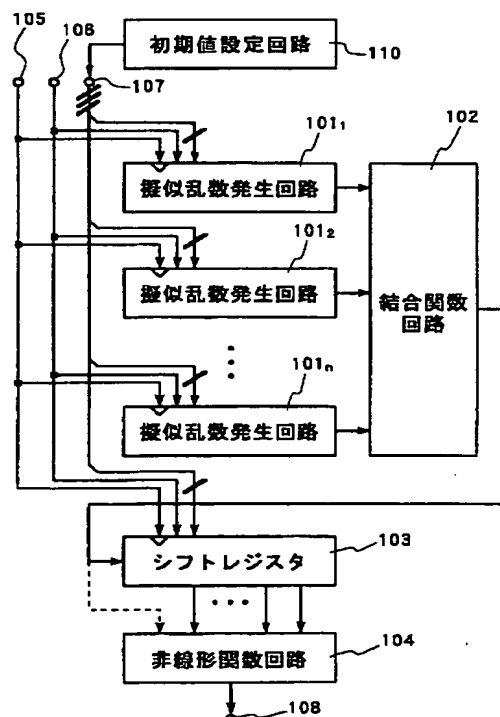
(74) 代理人 弁理士 若林 忠

(54) 【発明の名称】 擬似乱数発生装置

(57) 【要約】

【課題】 装置規模が小さくてすみ、線形フィードバック・シフトレジスタのみからなる少数の擬似乱数発生回路によって非線形性の大きな擬似乱数系列を発生でき、ストリーム暗号に適した擬似乱数発生装置を提供する。

【解決手段】 n 個の擬似乱数発生回路 $101_1 \sim 101_n$ と、これら n 個の擬似乱数発生回路 $101_1 \sim 101_n$ の出力を非線形結合してその結果を出力する結合関数回路 102 と、結合関数回路 102 の出力がシフト入力として入力するシフトレジスタ 103 と、シフトレジスタ 103 の内部状態のうち予め定められた複数のビットの非線形結合を計算する非線形関数回路 104 とを設け、非線形関数回路 104 での計算結果が擬似乱数を表わすビットストリームとして出力端子 108 から出力されるようにする。



【特許請求の範囲】

【請求項 1】 同一のクロックが入力し相互に同期して動作する複数の疑似乱数発生回路と、

前記各疑似乱数発生回路の出力を非線形関数で結合して出力する結合関数回路と、

前記クロックに同期して記憶内容を一端から他端に向う方向に 1 ビットずつシフトするとともに前記結合関数回路の出力を前記一端に記憶するシフトレジスタと、

前記シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路とを有し、

前記クロックに同期して前記非線形関数回路より疑似乱数を出力することを特徴とする疑似乱数発生装置。

【請求項 2】 同一のクロックが入力し相互に同期して動作する複数の疑似乱数発生回路と、

前記各疑似乱数発生回路の出力を非線形関数で結合して出力する結合関数回路と、

シフトレジスタと、

前記シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路と、

前記結合関数回路の出力と前記非線形関数回路の出力との排他的論理和を計算して出力する排他的論理和回路とを有し、

前記シフトレジスタは、前記クロックに同期して記憶内容を一端から他端に向う方向に 1 ビットずつシフトするとともに前記排他的論理和回路の出力を前記一端に記憶し、疑似乱数が前記クロックに同期して前記非線形関数回路より出力されることを特徴とする疑似乱数発生装置。

【請求項 3】 入力するクロックに同期して動作する単一の疑似乱数発生回路と、

シフトレジスタと、

前記シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路と、

前記疑似乱数発生回路の出力と前記非線形関数回路の出力との排他的論理和を計算して出力する排他的論理和回路とを有し、

前記シフトレジスタは、前記クロックに同期して記憶内容を一端から他端に向う方向に 1 ビットずつシフトするとともに前記排他的論理和回路の出力を前記一端に記憶し、疑似乱数が前記クロックに同期して前記非線形関数回路より出力されることを特徴とする疑似乱数発生装置。

【請求項 4】 前記疑似乱数発生回路と前記シフトレジスタに初期値を設定する初期値設定回路をさらに有する請求項 1 乃至 3 いずれか 1 項に記載の疑似乱数発生装置。

【請求項 5】 前記結合関数回路の出力も前記非線形関

数回路に入力し、前記非線形関数回路が前記シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値と前記結合関数回路の出力とを非線形結合して出力する請求項 1 または 2 に記載の疑似乱数発生装置。

【請求項 6】 前記疑似乱数発生回路が線形フィードバック・シフトレジスタである請求項 1 乃至 5 いずれか 1 項に記載の疑似乱数発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、疑似乱数を発生する疑似乱数発生装置に関し、特に、複数の疑似乱数発生回路を有しこれら疑似乱数発生回路の出力を非線形結合して疑似乱数を出力する疑似乱数発生装置に関する。

【0002】

【従来の技術】通信システムや計算機システムにおいては、許可されていない者が不正に情報を取得することなどを防止するために、情報に疑似乱数を排他的論理和で加算して暗号に変換したり、暗号に疑似乱数を排他的論理和で加算して元の情報を復元したりするストリーム暗号装置などが使用される。

【0003】情報への不正なアクセスを防ぐための暗号化に使用される疑似乱数は、以下に説明するように、非線形性が高いことが必須であり、そのため、暗号化に使用される疑似乱数の発生方法として、結合関数と呼ばれる非線形関数によって複数の疑似乱数発生回路の出力を非線形結合して非線形性のより高い疑似乱数を生成する方法が、従来より広く知られている。以下、疑似乱数発生回路とは、線形フィードバック・シフトレジスタなど、疑似乱数を与える基本的な回路のことを指し、疑似乱数発生装置とは、1 または複数の疑似乱数発生回路を含んでより非線形性の高い疑似乱数を発生する装置のことを言う。

【0004】ここで非線形結合とは、線形結合ではない結合のことである。ビット x_1, \dots, x_n, \dots の線形結合とは、 $y = x_1 + x_2 + \dots + x_n$ や $y = x_1 + x_2 + \dots + x_{n+1}$ など、排他的論理和 "+" だけを使ってビット y を与えることである。したがって、ビット x_1, \dots, x_n, \dots の非線形結合とは、 $y = x_1 * x_2 + x_2 * x_3 + \dots + x_n * x_1$ など、論理積 "*" と排他的論理和 "+" の両方（否定論理を含んでもよい）を使ってビット y を与えることであり、 y を与える式をどのように変形しても線形結合に帰着しないようなものである。また、非線形結合の非線形性とは、 y を与える式の次数のことであり、式の次数が大きいほど非線形性が高いとされる。なお、非線形関数の入力（結合されるべき疑似乱数発生回路の数）を増やすほど、非線形性の高い非線形結合が実現可能になる。

【0005】図 4 は、従来の疑似乱数発生装置の一例の構成を示す機能ブロック図である。この疑似乱数発生装置は n 個の疑似乱数発生回路 $401_1 \sim 401_n$ と、これら n 個の疑似乱数発生回路 $401_1 \sim 401_n$ の出力を非

線形結合して擬似乱数を出力端子408から出力する結合関数回路402と、制御パルス（クロック）が入力する入力端子405と、モード制御用の入力端子406と、初期状態と呼ばれるビット系列を入力するための入力端子407とから構成されている。n個の擬似乱数発生回路401₁～401_nは、いずれも、入力端子405～407に接続しており、入力端子406に"0"が供給されている時に入力端子405に制御パルスが入力された場合には、入力端子407から供給される初期状態を取り込んで内部状態として保持し、入力端子406に"1"が供給されている場合には、入力端子405に制御パルスが1個入力されるごとに擬似乱数を出力するように構成されている。なお、擬似乱数発生回路401₁～401_nには、一般に、それぞれ異なる初期状態が供給される。

【0006】図4の擬似乱数発生装置を用いて擬似乱数を発生させる場合には、まず、入力端子407に初期状態を供給し、次に、入力端子406に"0"を供給して、入力端子405に制御パルスを1個入力する。そして、入力端子406に"1"を供給する。するとそれ以降は、入力端子405に制御パルスを1個入力するごとに、各擬似乱数発生回路401₁～401_nの出力を結合関数回路402によって非線形結合して得られた擬似乱数が、出力端子408から得られる。

【0007】しかしながら、図4に示す擬似乱数発生装置は、しばしば、各擬似乱数発生回路401₁～401_nに設定された初期状態がコリレーション・アタックと呼ばれる解読方法によって推定されてしまい、その結果、暗号の不正な解読を許してしまうという問題点がある。すなわち、ある擬似乱数発生回路401_j（1≦j≦n）の出力で条件付けたときの結合関数回路402の出力の条件付き確率分布が一樣でない場合には、その擬似乱数発生回路401_jと等価な擬似乱数系列発生回路を想定し、この擬似乱数系列発生回路の出力系列と結合関数回路402の出力系列との相関が最大になるようにその擬似乱数系列発生回路の初期状態を求めることで、擬似乱数発生回路401_jに与えられた初期状態を知ることができる。このような性質があると、ストリーム暗号の擬似乱数発生装置としては使えない。なお、コリレーション・アタックに関しては、R. A. Rueppel（ルエペル）著、"Analysis and Design of Stream Ciphers（アナリシス・アンド・デザイン・オブ・ストリーム・サイファーズ）"、Springer-Verlag（スプリングァー・ヴァーラグ）社、1986年の第92頁から第141頁にその詳しい解説がある。

【0008】そこで本発明者は、コリレーション・アタックによる解読を防ぐために、特開平7-104976号公報において、結合関数回路が出力するビットストリームをそのまま擬似乱数として使うのではなく、結合関数回路の出力を畳み込んで得られるビットストリームを

擬似乱数として用いる擬似乱数発生装置を提案した。そのようにすれば、ある擬似乱数発生回路の出力で条件付けたときの擬似乱数の条件付き確率分布がほぼ一樣になり、コリレーション・アタックが困難になる。

【0009】図5は、コリレーション・アタック対策を施した従来の擬似乱数発生装置の一例を示す機能ブロック図である。この擬似乱数発生装置は、図4に示す擬似乱数発生装置において、結合関数回路402と出力端子408との間に、シフトレジスタ410と排他的論理和回路411を挿入した構成である。シフトレジスタ410は、入力端子405～407にも接続しており、入力端子406に"0"が供給されている時に入力端子405に制御パルスが入力すると、入力端子407から供給されている初期状態と呼ばれるビット系列を内部状態として保持し、入力端子406に"1"が供給されている場合には、入力端子405に制御パルスが1個入力されるごとに、内部状態を1ビットだけ右にシフトし、左端のビットに結合関数回路402の出力を保持するように構成されている。また、排他的論理和回路411は、シフトレジスタ410の内部状態のうち予め決められた複数のビットの線形結合を計算するものであり、その計算結果が擬似乱数として出力端子408から出力される。なお、図示点線で示されるように、結合関数回路402の出力も排他的論理和回路411に入力するようにしてもよい。

【0010】図5に示す擬似乱数発生装置を用いて擬似乱数を発生させる場合には、まず、入力端子407に初期状態を供給し、次いで入力端子406に"0"を供給して、入力端子405に制御パルスを1個入力する。そして、入力端子406に"1"を供給する。するとそれ以降は、入力端子405に制御パルスを1個入力するごとに、出力端子408から擬似乱数が得られる。

【0011】図6は、シフトレジスタ410の内部構成を示す回路図である。このシフトレジスタ410はm段構成であり、クロック入力端子415と、モード切り換え信号入力端子416と、このシフトレジスタ410に内部状態を設定するための内部状態入力端子417と、このシフトレジスタ410の内部状態を出力するための内部状態出力端子418と、シフト入力端子419と、モード切り換え信号入力端子416に入力した信号に応じて選択動作を行うm個の2入力セクタ421₁～421_mと、クロック入力端子415に入力した信号をクロックとしセクタ421₁～421_mの出力をそれぞれ入力とするm個のD型フリップフロップ422₁～422_mによって構成されている。なお、D型フリップフロップ422₁～422_mの出力系列のことをこのシフトレジスタ410の内部状態という。図5に示される状態では、このシフトレジスタのクロック入力端子415は入力端子405に接続し、モード切り換え信号入力端子416は入力端子406に接続し、内部状態入力端子41

7は入力端子407に接続し、シフト入力端子419は結合関数回路402の出力に接続している。

【0012】図示左端のセクタ421₁には、シフト入力端子419を介して結合関数回路402（図5参照）が入力するとともに、内部状態入力端子417から入力した内部状態のうちの1ビットが入力する。その他のセクタ421_j（ $j=2, \dots, m$ ）には、それぞれ、D型フリップフロップ421_{j-1}の出力と、内部状態入力端子417から入力した内部状態のうちのそれぞれに固有の1ビットとが入力する。そして、各セクタ421₁～421_mは、モード切り換え信号入力端子416から"0"が供給されている時に、それぞれ内部状態入力端子417から供給されるビットを選択して出力し、モード切り換え信号入力端子416から"1"が供給されているときには、シフト入力端子419や前段のD型フリップフロップ422₁～422_{m-1}から入力する信号を選択して出力する。各D型フリップフロップ422₁～422_mは、クロック入力端子415から制御パルスが1個入るごとに、それぞれ、セクタ421₁～421_mの出力を保持して、保持している値を出力する。これらD型フリップフロップ422₁～422_mの出力は、mビット並列に、内部状態出力端子418から出力され、これらのうちのいくつかのビットが排他的論理和回路411（図5参照）に入力する。

【0013】次に、各擬似乱数発生回路401₁～401_nの構成について説明する。擬似乱数発生回路401₁～401_nとしては、例えば、図7に示すように線形フィードバック・シフトレジスタのみで構成された擬似乱数発生回路501を使用することもできるし、図8に示すように非線形関数回路と線形フィードバック・シフトレジスタを組み合わせた擬似乱数発生回路511を使用することもできるし、さらにはここで述べるのとは異なる回路構成のものも使用することもできる。

【0014】まず、図7を用いて線形フィードバック・シフトレジスタのみからなる擬似乱数発生回路501を説明する。この擬似乱数発生回路501は、シフトレジスタ502と排他的論理和回路503とから構成されている。シフトレジスタ502は、段数は異なってもよいが図6に示すシフトレジスタ410と同様の構造を持つものである。シフトレジスタ502のクロック入力端子、モード切り換え信号入力端子、内部状態入力端子（いずれも図6参照）は、それぞれ、入力端子405、406、407に接続している。そして、シフトレジスタ502の内部状態出力端子（図6参照）からの出力のうち予め決められたビットだけが排他的論理和回路503に供給され、排他的論理和回路503の出力が、出力端子504から出力されるとともに、シフトレジスタ502のシフト入力端子（図6）に供給されている。なお、排他的論理和回路503は、入力された各ビットのデータの排他的論理和を計算して、その結果を出力する

ものである。

【0015】図7に示す擬似乱数発生回路501は、いわゆるM系列発生回路であり、この回路単独で発生させた擬似乱数のランダム性はあまり良くなく、また、初期状態を容易に推定することができるので、単独では暗号化のために使用することには適さない。

【0016】図8に示す擬似乱数発生回路511は、シフトレジスタ512と排他的論理和回路513の他に、非線形関数回路514を有している。シフトレジスタ512は、段数は異なってもよいが図6に示すシフトレジスタ410と同様の構造を持つものである。シフトレジスタ512のクロック入力端子、モード切り換え信号入力端子、内部状態入力端子（いずれも図6参照）は、入力端子405、406、407に接続している。そして、シフトレジスタ512の内部状態出力端子（図6参照）からの出力のうち予め決められたビットが排他的論理和回路513に供給されて、排他的論理和回路513の出力がシフトレジスタ512のシフト入力端子（図6）に供給されている。なお、排他的論理和回路513は、入力された各ビットのデータの排他的論理和を計算して、その結果を出力するものである。さらに、シフトレジスタ512の内部状態出力端子からの出力の全ビットあるいは予め定められたビットが非線形関数回路514に入力して非線形結合され、この非線形結合された結果が擬似乱数として出力端子515から出力される。

【0017】次に、結合関数について説明する。結合関数とは、既に述べたように、入力されたビットの非線形結合をとって、その結果を出力するものである。結合関数を出力する結合関数回路は、論理関数回路やリード・オンリ・メモリあるいはそれらの組合せによって実現できる。図9は3入力の結合関数回路450を示す機能ブロック図である。すなわちこの結合関数回路450は、図4や図5の擬似乱数発生装置において $N=3$ （擬似乱数発生回路の数が3個）の場合に、結合関数回路402として使用できるものである。

【0018】この結合関数回路は、否定回路451と、2つの2入力論理積回路452、453と、2入力排他的論理和回路454と、それぞれ異なる擬似乱数発生回路が発生する擬似乱数が入力する3個の入力端子455₁～455₃と、排他的論理和回路454の出力に接続された出力端子458とによって構成されている。第1の入力端子455₁に入力した擬似乱数は第1の論理積回路452の一方の入力に供給され、第2の入力端子455₂に入力した擬似乱数は第1の論理積回路452の他方の入力と否定回路451に供給される。第2の論理積回路453には、第3の入力端子455₃に入力した擬似乱数と、否定回路451で反転された第2の入力端子455₂からの擬似乱数が入力する。そして、各論理積回路452、453は、それぞれへの入力の論理積を計算して結果を排他的論理和回路454に出力し、排他的

論理和回路454は、第1の論理積回路452の出力と第2の論理積回路453の出力の排他的論理和を計算してその結果を出力端子458から出力する。

【0019】

【発明が解決しようとする課題】以上、従来の擬似乱数発生装置についてやや詳しく説明したが、上述の従来の擬似乱数発生装置には、回路規模を小さくしようとする非線形性の小さい擬似乱数しか生成できず、一方、非線形性の大きな擬似乱数を発生させようとする装置規模が大きくなるという問題点がある。すなわち、回路規模を小さくするためには、擬似乱数発生回路として線形フィードバック・シフトレジスタのみからなるものを使用することが有効であるが、そうすると、非線形変換を行うのが結合関数回路だけとなり、非線形性の大きな擬似乱数を得ることができなくなる。また、回路規模を小さくするために擬似乱数発生回路の個数自体を減らした場合には、結合関数への入力数が減ることとなって結合関数の非線形性が小さくなり、非線形性がさらに小さな擬似乱数しか得られなくなる。逆に、得られる擬似乱数の非線形性を大きくするためには擬似乱数発生回路として非線形関数回路と線形フィードバック・シフトレジスタを組み合わせるものを用いることが有効であるが、そうすると、非線形関数回路を実現するための複雑な論理回路やリード・オンリ・メモリ（ROM）が擬似乱数発生回路の個数だけ必要になってしまい、回路規模が必然的に大きくなる。また、擬似乱数の非線形性を大きくするために結合関数への入力数を増やすと、その分、擬似乱数発生回路の数も増やさなければならない。

【0020】本発明の目的は、上述した従来の擬似乱数発生装置の抱える問題点を解決し、線形フィードバック・シフトレジスタのみからなる少数の擬似乱数発生回路によって非線形性の大きな擬似乱数系列を発生でき、ストリーム暗号に適した擬似乱数発生装置を提供することにある。

【0021】

【課題を解決するための手段】本発明の第1の擬似乱数発生装置は、同一のクロックが入力し相互に同期して動作する複数の擬似乱数発生回路と、各擬似乱数発生回路の出力を非線形関数で結合して出力する結合関数回路と、クロックに同期して記憶内容を一端から他端に向う方向に1ビットずつシフトするとともに結合関数回路の出力を一端に記憶するシフトレジスタと、シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路とを有し、クロックに同期して非線形関数回路より擬似乱数を出力する。

【0022】本発明の第2の擬似乱数発生装置は、同一のクロックが入力し相互に同期して動作する複数の擬似乱数発生回路と、各擬似乱数発生回路の出力を非線形関数で結合して出力する結合関数回路と、シフトレジスタと、シフトレジスタの記憶ビットのうち所定の複数の記

憶ビットの値を非線形結合して出力する非線形関数回路と、結合関数回路の出力と非線形関数回路の出力との排他的論理和を計算して出力する排他的論理和回路とを有し、シフトレジスタは、クロックに同期して記憶内容を一端から他端に向う方向に1ビットずつシフトするとともに排他的論理和回路の出力を一端に記憶し、擬似乱数がクロックに同期して非線形関数回路より出力される。

【0023】本発明の第3の擬似乱数発生装置は、入力するクロックに同期して動作する単一の擬似乱数発生回路と、シフトレジスタと、シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値を非線形結合して出力する非線形関数回路と、擬似乱数発生回路の出力と非線形関数回路の出力との排他的論理和を計算して出力する排他的論理和回路とを有し、シフトレジスタは、クロックに同期して記憶内容を一端から他端に向う方向に1ビットずつシフトするとともに排他的論理和回路の出力を一端に記憶し、擬似乱数がクロックに同期して非線形関数回路より出力される。

【0024】本発明においては、擬似乱数発生回路として、線形フィードバック・シフトレジスタを好ましく使用できる。また、擬似乱数発生回路とシフトレジスタに初期値を設定する初期値設定回路を設けるようにするよい。さらに、結合関数回路の出力も非線形関数回路に入力し、非線形関数回路によって、シフトレジスタの記憶ビットのうち所定の複数の記憶ビットの値と結合関数回路の出力とが非線形結合して出力されるようにしてもよい。

【0025】以下、本発明についてさらに詳しく説明する。

【0026】図5に示す従来の擬似乱数発生装置では、結合関数回路402の出力系列をシフトレジスタ410に保持し、シフトレジスタ410の内部状態のすべてあるいは予め決められた一部のビットを排他的論理和回路411によって線形結合して擬似乱数を生成していた。このように構成すると、ある擬似乱数発生回路401

($1 \leq j \leq N$)の出力で条件付けたときの擬似乱数の条件付き確率分布がほぼ一樣になるため、コリレーション・アタックが困難になる。このような手法は、物理的な方法で発生される乱数（例えば、サイコロを振って決められる乱数）の分布を一樣にする目的でも、長年にわたって用いられてきた。このため、コリレーション・アタックを防ぐためには、線形結合が有用だと考えられていた。

【0027】しかしながら、線形結合によって条件付き確率が一樣になるのは、線形結合の線形性によるものではなく、線形結合の一樣性によるものである。ここで、一樣とは、ランダムに与えられたビットを結合することにより、ほぼ等確率に"0"と"1"を生ずることである。したがって、一樣な非線形結合であれば、線形結合の代りに用いても、コリレーション・アタックを防ぐことが

可能なはずである。

【0028】そこで本発明では、図5に示す従来の擬似乱数発生装置における排他的論理和回路の代りに、一様な非線形結合を行う非線形関数回路を使用し、結合関数回路の出力が入力するシフトレジスタの内部状態をこの非線形関数回路によって非線形結合して擬似乱数として出力する。このように構成することにより、コリレーション・アタックを防ぐという性質を保ったまま、擬似乱数の非線形性を高められる。さらに本発明では、結合関数回路とシフトレジスタとの間に排他的論理和回路を設け、非線形関数回路の出力と結合関数回路の出力を排他的論理和で足し込んだものがシフトレジスタに入力するように構成することができる。このように構成すると、非線形関数回路の出力がシフトレジスタにフィードバックされることになり、非線形関数回路で行われる非線形結合の非線形性が小さい場合であっても、 x の2乗が x^2 に、その2乗が x^4 に、さらにその2乗が x^8 にという具合に非線形性の低い変換の繰り返しが非線形性の高い変換に帰着することから、非線形性がさらに高められた擬似乱数を得ることが可能になる。

【0029】

【発明の実施の形態】次に、本発明の実施の形態について、図面を参照して説明する。

【0030】《第1の実施の形態》図1は、本発明の第1の実施の形態の擬似乱数発生装置の構成を示す機能ブロック図である。この擬似乱数発生装置は、 n 個の擬似乱数発生回路101₁～101_nと、これら n 個の擬似乱数発生回路101₁～101_nの出力を非線形結合してその結果を出力する結合関数回路102と、結合関数回路102の出力がシフト入力として入力するシフトレジスタ103と、シフトレジスタ103の内部状態のうち予め定められた複数のビット（シフトレジスタ103の全記憶ビットでもよい）の非線形結合を計算する非線形関数回路104と、制御パルス（クロック）が入力する入力端子105と、モード制御用の入力端子106と、初期状態と呼ばれるビット系列を入力するための入力端子107とを有し、非線形関数回路104での計算結果が擬似乱数を表わすビットストリームとしてクロックに同期して出力端子108から出力されるように構成されている。なお、図示点線で示されるように、結合関数回路102の出力も非線形関数回路104に入力するようにしてもよい。

【0031】 n 個の擬似乱数発生回路101₁～101_nは、いずれも、入力端子105～107に接続しており、入力端子106に"0"が供給されている時に入力端子105に制御パルスが入力された場合には、入力端子107から供給される初期状態を取り込んで内部状態として保持し、入力端子106に"1"が供給されている場合には、入力端子105に制御パルスが1個入力されるごとに擬似乱数を出力する。この擬似乱数発生回路10

1₁～101_nとしては、上述の図7に示したような線形フィードバック・シフトレジスタのみからなるものを好ましく使用できる。また、シフトレジスタ104は、入力端子105～107にも接続しており、入力端子106に"0"が供給されている時に入力端子105に制御パルスが入力すると、入力端子107から供給されている初期状態と呼ばれるビット系列を内部状態として保持し、入力端子106に"1"が供給されている場合には、入力端子105に制御パルスが1個入力されるごとに、内部状態を1ビットだけ右にシフトし、左端のビットに結合関数回路102の出力を保持するように構成されている。シフトレジスタ104としては、例えば、上述の図6に示す構成のものを使用することができる。

【0032】上述の説明から明らかなように、擬似乱数発生回路101₁～101_n、結合関数回路102、入力端子105～107は、それぞれ、図4及び図5における擬似乱数発生回路401₁～401_n、結合関数回路402、入力端子405～407に対応し、シフトレジスタ103は、図5のシフトレジスタ410に対応する。また、結合関数回路102と非線形関数回路104は、この分野での慣例に従って別の名称で呼んでいるが、どちらも非線形結合を行う回路であるという点では同様のものである（入力ビット数や内部構造は異なるかもしれない）。

【0033】非線形関数回路104としては、一様な非線形結合を行う回路であれば任意のものを使用できる。例えば、リード・オンリ・メモリ（ROM）を用いたルック・アップ・テーブル形式の構成とすることができる。具体的には、図10(a)に示すように、ROM151に"0"と"1"とを個数が等しくなるように書き込んでおき、非線形関数回路104に対する複数の入力をこのROM151の複数のアドレス入力端子それぞれへのアドレス入力とみて、このROM151からの1ビットのデータ出力を非線形関数回路104の出力とするような構成とすることができる。非線形関数回路104の入力数、すなわちROMに対する入力ビット数が増えた場合には、1個のROMを用いたのでは実現できなくなるが、そのような場合には、図10(b)に示すように、上述したROM151を複数用意してこれらROM151の出力を排他的論理和回路152に入力し、この排他的論理和回路152の出力を非線形関数回路104の出力とするように構成すればよい。

【0034】なお、擬似乱数発生回路101₁～101_n及びシフトレジスタ103には、入力端子107を介して一般に、それぞれ異なる初期状態が供給される。各擬似乱数発生回路101₁～101_nやシフトレジスタ103に供給される初期状態は、それぞれ、それらの内部ビット幅に応じて複数のビットであるから、入力端子107のビット幅は、これら擬似乱数発生回路101₁～101_nやシフトレジスタ103の内部ビット幅の総和と

なるようにするとよい。あるいは、内部状態設定のための制御が個別に行えるような構成とするよい。図示した例では、各擬似乱数発生回路 101₁~101_n及びシフトレジスタ 103 に初期状態のビット系列を設定するために、入力端子 107 に、これら擬似乱数発生回路 101₁~101_nやシフトレジスタ 103 の初期状態を発生する初期状態設定回路 110 が接続されている。

【0035】この擬似乱数発生装置を用いて擬似乱数を発生させる場合には、まず、擬似乱数発生回路 101₁~101_n及びシフトレジスタ 103 の初期状態を初期値設定回路 110 によって入力端子 107 に供給する。次いで、入力端子 106 に“0”を供給して入力端子 105 に制御パルスを 1 個入力する。その結果、各擬似乱数発生回路 101₁~101_n及びシフトレジスタ 103 に初期状態が設定される。そして、入力端子 106 に“1”を供給すると、それ以降は、入力端子 105 に制御パルスを 1 個入力するごとに、出力端子 108 から 1 ビットずつ擬似乱数が得られる。

【0036】《第 2 の実施の形態》次に、本発明の第 2 の実施の形態について、図 2 を用いて説明する。図 2 に示す擬似乱数発生装置は、図 1 に示すものと比べ、結合関数回路 102 とシフトレジスタ 103 との間に排他的論理和回路 111 が挿入され、シフトレジスタ 103 のシフト入力には、結合関数回路 102 の出力ではなく排他的論理和回路 111 の出力が入力する点で異なっている。排他的論理和回路 111 は、結合関数回路 102 の出力と非線形関数回路 104 の出力との排他的論理和を求めて出力する。この擬似乱数発生装置では、排他的論理和回路 111 を介して非線形関数回路 104 の出力がシフトレジスタ 103 にフィードバックされるので、非線形関数回路 104 の非線形性が小さい場合であっても、非線形性の大きな擬似乱数を出力端子 108 から得ることができる。この擬似乱数発生装置を用いて擬似乱数を発生させるときの手順は、図 1 に示す擬似乱数発生装置での手順と同じである。

【0037】《第 3 の実施の形態》上述の各実施の形態の擬似乱数発生装置は、出力端子 108 に接続する非線形関数回路 104 によって非線形性を高めているので、特に第 2 の実施の形態のように非線形関数回路 104 の出力をシフトレジスタ 103 にフィードバックさせる場合には、擬似乱数発生回路の個数を 1 個としても、十分に非線形性の高い擬似乱数を得ることができる。図 3 は、このような構成の擬似乱数発生装置を示している。この擬似乱数発生装置では、単一の擬似乱数発生回路 101 が設けられている。擬似乱数発生回路が 1 個なので結合関数回路は不要であり、この擬似乱数発生回路 101 の出力がそのまま排他的論理和回路 111 に入力している。その他の構成や擬似乱数発生のための手順は第 2 の実施の形態におけるものと同様である。

【0038】

【発明の効果】以上説明したように本発明は、ある擬似乱数発生回路の出力で条件付けたときの擬似乱数の条件付き確率分布を一様にするために、線形結合回路でなく一様な非線形結合を行う非線形関数回路を使用しているので、擬似乱数の非線形性が高められ、コリレーション・アタックに強い擬似乱数を発生でき、ストリーム暗号に適した擬似乱数発生装置が実現できるという効果がある。また、擬似乱数発生回路として単純な線形フィードバック・シフトレジスタを使用しても擬似乱数の非線形性が高いので、小規模な装置で非線形性の高い擬似乱数を発生できるようになり、擬似乱数発生装置を低コストで実現できるようになる。

【0039】また、非線形関数回路の出力が排他的論理和回路を介してシフトレジスタにフィードバックするように構成した場合には、非線形変換の繰返しが行われることによって、非線形関数回路の非線形性が小さい場合でも非線形性のより大きな擬似乱数を生成できるようになり、したがって、非線形関数回路の規模を小さくすることができるようになる。

【図面の簡単な説明】

【図 1】本発明の第 1 の実施の形態の擬似乱数発生装置の構成を示す機能ブロック図である。

【図 2】本発明の第 2 の実施の形態の擬似乱数発生装置の構成を示す機能ブロック図である。

【図 3】本発明の第 3 の実施の形態の擬似乱数発生装置の構成を示す機能ブロック図である。

【図 4】従来の擬似乱数発生装置の一例を示す機能ブロック図である。

【図 5】コリレーション・アタック対策の施された従来の擬似乱数発生装置の一例を示す機能ブロック図である。

【図 6】シフトレジスタの構成例を示す回路図である。

【図 7】線形フィードバック・シフトレジスタを利用した擬似乱数発生回路を示す機能ブロック図である。

【図 8】非線形関数回路と線形フィードバック・シフトレジスタを利用した擬似乱数発生回路を示す機能ブロック図である。

【図 9】3 入力の結合関数回路を示す回路図である。

【図 10】(a)、(b)は、それぞれ、非線形関数回路の構成例を示す回路図である。

【符号の説明】

101, 101₁~101_n, 401₁~401_n 擬似乱数発生回路

102, 402, 450 結合関数回路

103, 403, 410, 502, 512 シフトレジスタ

104, 514 非線形関数回路

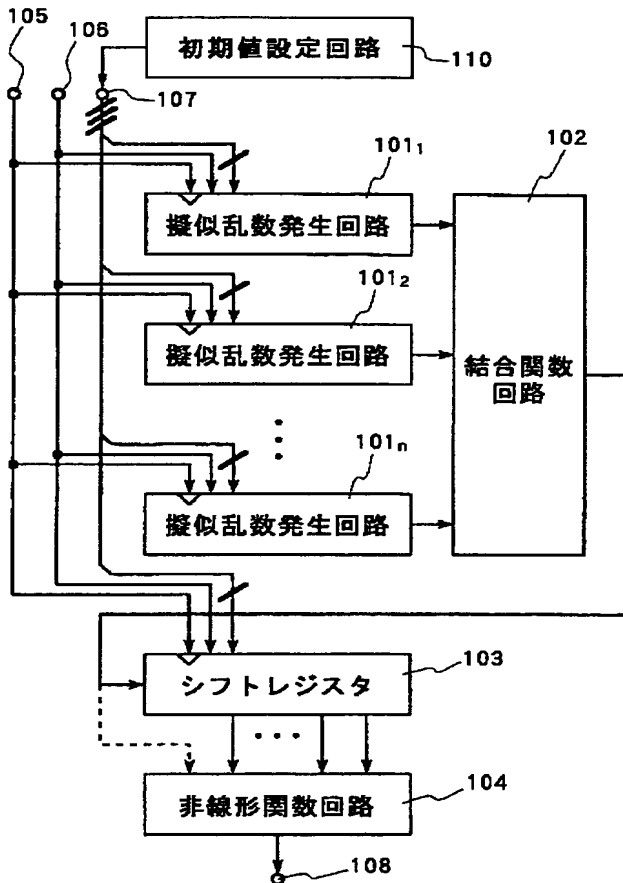
105~107, 405~407 入力端子

108, 408 出力端子

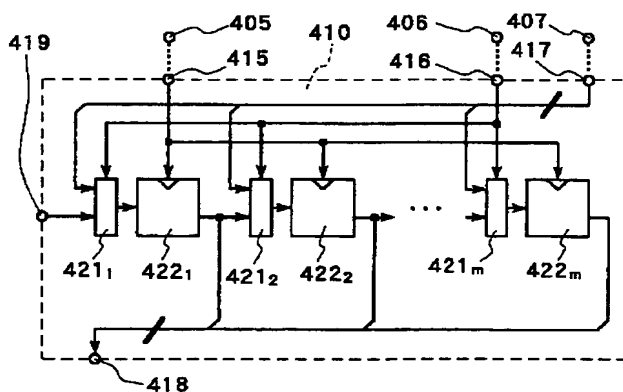
110 初期値発生回路

151 ROM
 111, 152, 411, 454, 503, 513 排他
 的論理回路
 415 クロック入力端子
 416 モード切り換え信号入力端子
 417 内部状態入力端子

【図1】

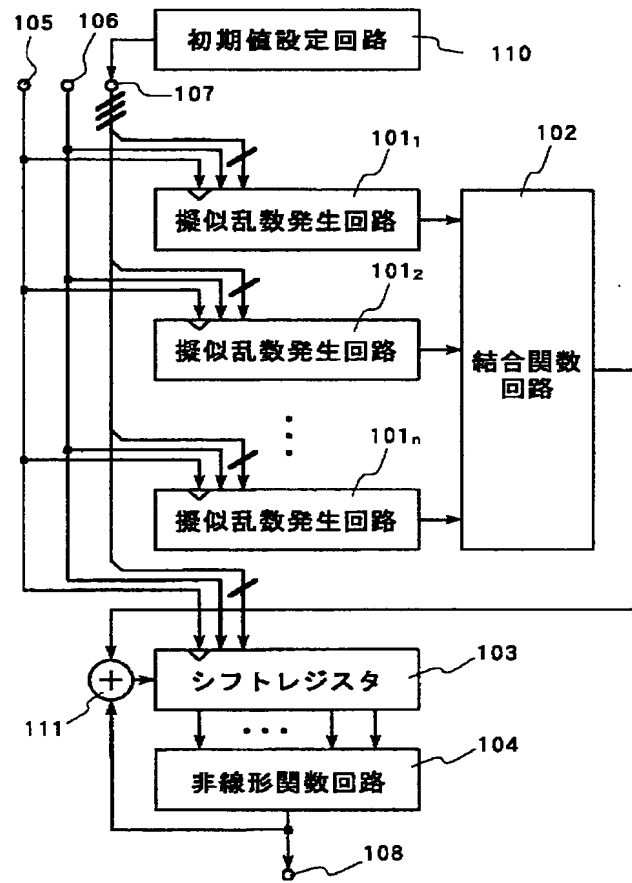


【図6】

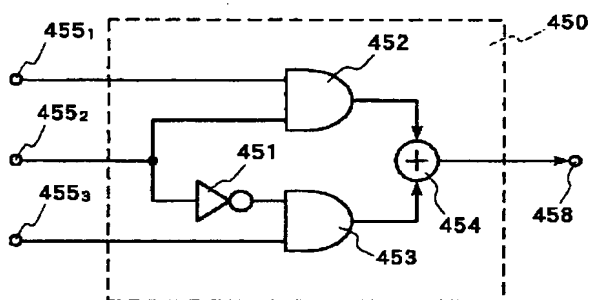


418 内部状態出力端子
 419 シフト入力端子
 421₁ ~ 421_m セレクタ
 422₁ ~ 422_m D型フリップフロップ
 451 否定回路
 453, 453 論理積回路

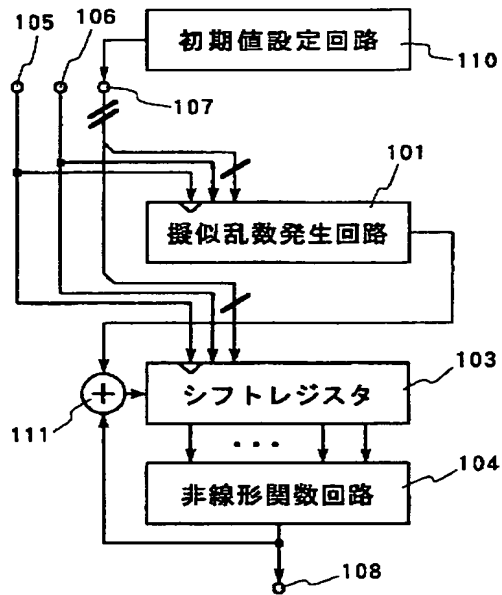
【図2】



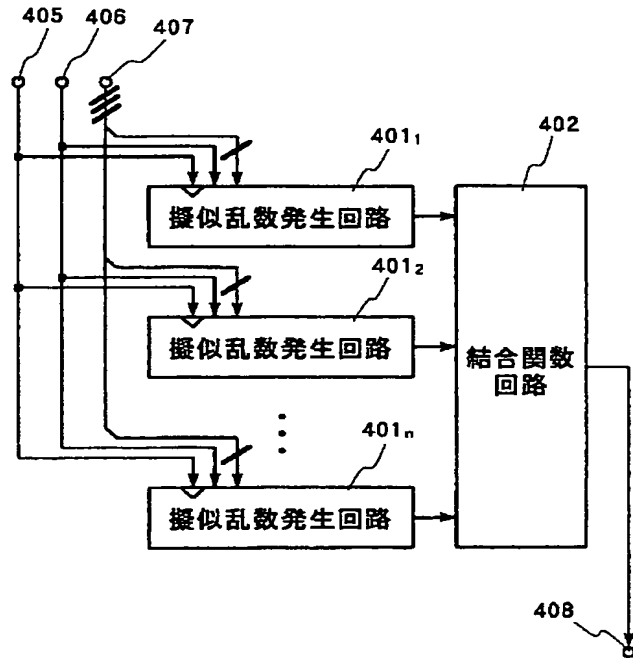
【図9】



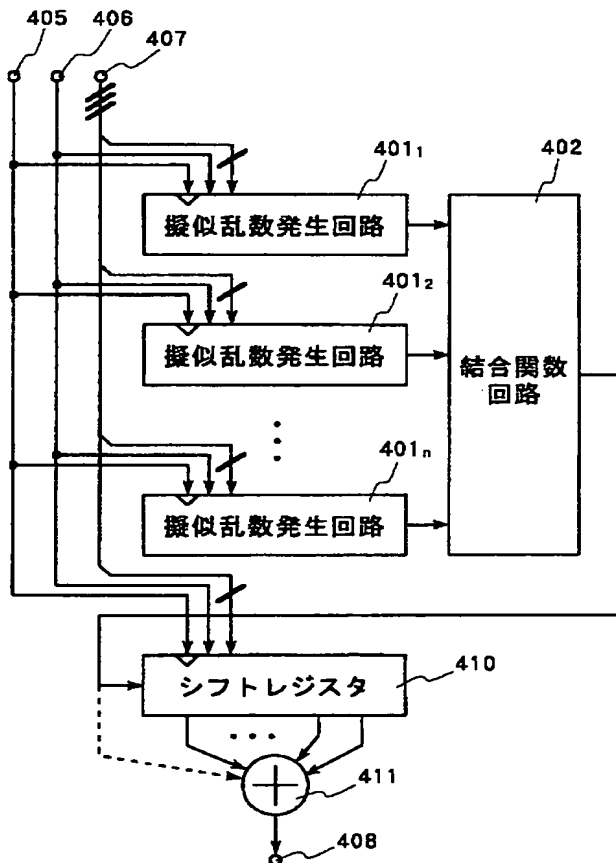
【図3】



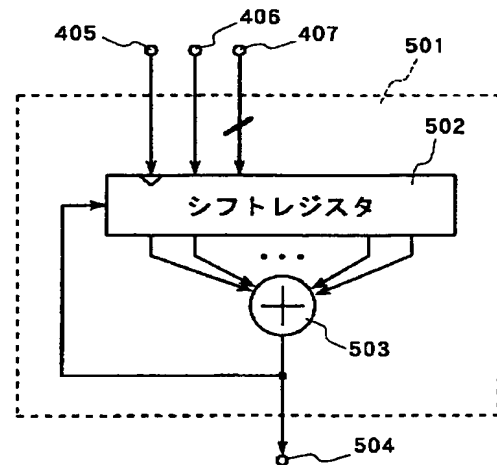
【図4】



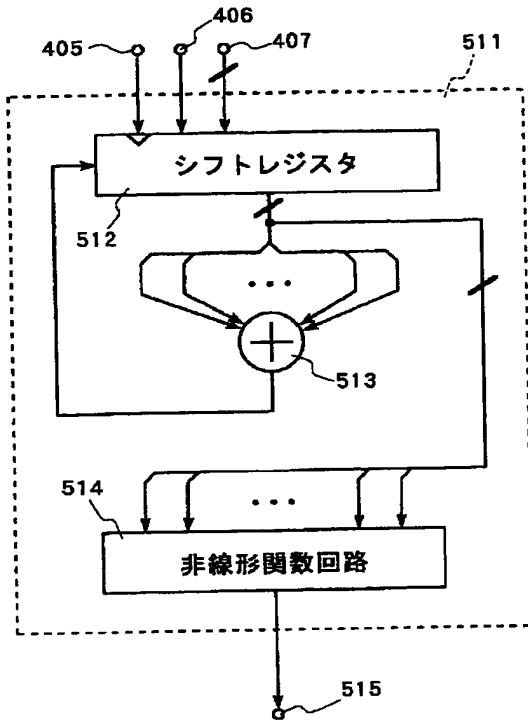
【図5】



【図7】



【図 8】



【図 10】

